UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

BARBARA MILLER, on behalf of herself and all others similarly situated, Plaintiff, v. NELNET SERVICING, LLC., Defendant.	Case No. CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff, Barbara Miller ("Ms. Miller" or "Plaintiff"), brings this action on behalf of herself and all others similarly situated against Defendant, Nelnet Servicing, LLC ("Nelnet" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities, and alleges as follows:

INTRODUCTION

1. Nelnet, a student loan servicing company, lost control over millions of borrowers' highly sensitive personal information in a data breach by cybercriminals ("Data Breach"). Starting in June 2022, an unauthorized third party gained access to Nelnet's student loan account registration information.

2. The compromised information included consumers' "personally identifiable information" ("PII"), including names, addresses, email addresses, phone numbers and Social Security numbers.

3. On information and belief, Nelnet first identified unusual activity on its network on or about July 22, 2022, and later concluded the Data Breach had begun more than a month earlier –on or about June 1, 2022.

4. On information and belief, cybercriminals bypassed Defendant's inadequate security systems to access borrowers' PII in its computer systems.

5. On or around August 26, 2022—over a month after Nelnet first discovered the Data Breach—Nelnet finally began notifying victims about the breach.

6. Defendant's Breach Notice obfuscated the nature of the breach and the threat it posed—refusing to tell its consumers how many people were impacted, how the breach happened, or why it took the Defendant over a month to begin notifying victims that hackers had gained access to borrowers' highly sensitive information.

7. Defendant's failure to timely detect and report the Data Breach made borrowers vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

8. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

9. In failing to adequately protect consumers' information, adequately notify them about the breach, and obfuscating the nature of the breach, Defendant violated applicable law and harmed thousands of borrowers across the country.

10. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the

proposed Class trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

11. Ms. Miller had a student loan through EdFinancial that was serviced by Nelnet. Ms. Miller received a Breach Notice on or about August 29, 2022.

12. Accordingly, Plaintiff, on her own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

PARTIES

13. Plaintiff, Barbara Miller, is a natural person and citizen of Minnesota, residing in St. Paul, Minnesota, where she intends to remain. Miller is a Data Breach victim, receiving Nelnet's Breach Notice on August 29, 2022.

14. Defendant, Nelnet is a Nebraska limited liability company with its principal place of business at 121 S. 13th Street, Suite 100, Lincoln, NE 68508. Nelnet is a wholly owned subsidiary of Nelnet Inc., a Nebraska corporation.

JURISDICTION & VENUE

15. This Court has subject-matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

16. This Court has general personal jurisdiction over Nelnet because it is incorporated in Nebraska and its principal place of business is in Nebraska.

17. Venue is proper in this Court because Nelnet is headquartered in this District.

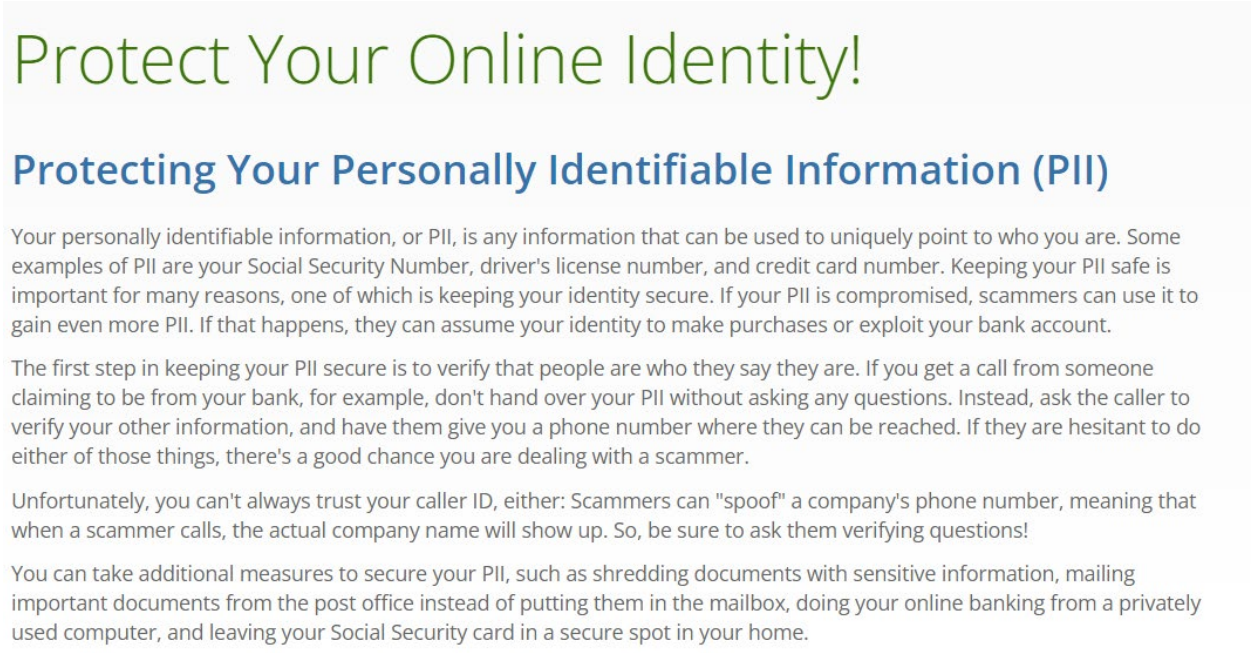
BACKGROUND FACTS

Nelnet

18. Nelnet describes itself as "much more" than a student loan servicing company.[1] Nelnet additionally provides services in consumer finance, telecommunications, K-12 and higher education. Nelnet has more than 8,5000 employees around the world.

19. As a servicer of student loans, Nelnet accumulates highly sensitive PII of student loan borrowers.

20. Nelnet understands PII must be protected. Nelnet's website urges consumers to "Protect your Online Identity" and offers advice on how to protect PII[2]:



Protect Your Online Identity!

Protecting Your Personally Identifiable Information (PII)

Your personally identifiable information, or PII, is any information that can be used to uniquely point to who you are. Some examples of PII are your Social Security Number, driver's license number, and credit card number. Keeping your PII safe is important for many reasons, one of which is keeping your identity secure. If your PII is compromised, scammers can use it to gain even more PII. If that happens, they can assume your identity to make purchases or exploit your bank account.

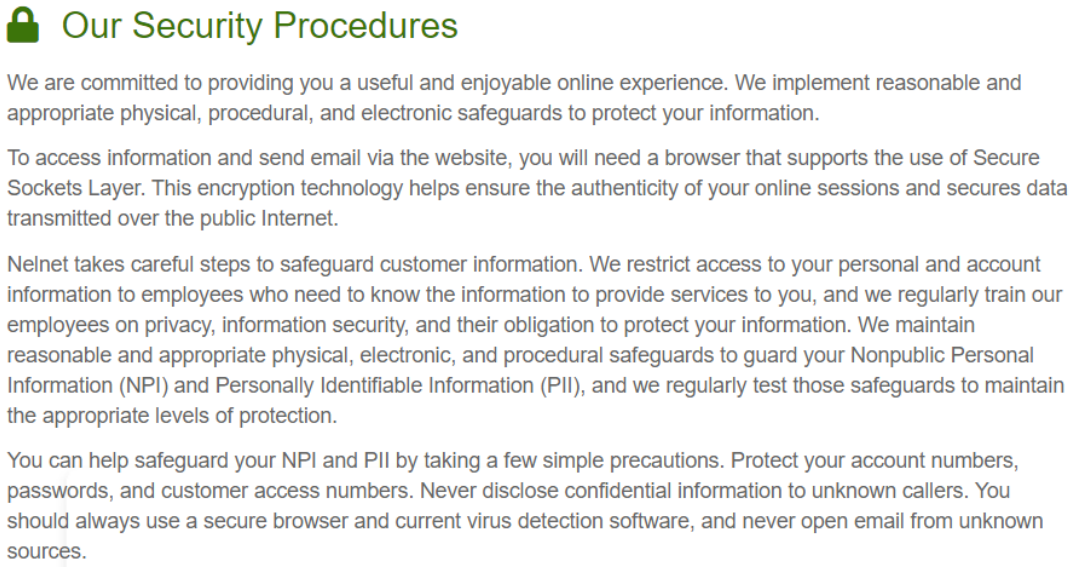
The first step in keeping your PII secure is to verify that people are who they say they are. If you get a call from someone claiming to be from your bank, for example, don't hand over your PII without asking any questions. Instead, ask the caller to verify your other information, and have them give you a phone number where they can be reached. If they are hesitant to do either of those things, there's a good chance you are dealing with a scammer.

Unfortunately, you can't always trust your caller ID, either: Scammers can "spoof" a company's phone number, meaning that when a scammer calls, the actual company name will show up. So, be sure to ask them verifying questions!

You can take additional measures to secure your PII, such as shredding documents with sensitive information, mailing important documents from the post office instead of putting them in the mailbox, doing your online banking from a privately used computer, and leaving your Social Security card in a secure spot in your home.

21. Nelnet publicly states that it "takes careful steps to safeguard customer information" including consumer training and physical, electronic and procedural safeguards:[3]

[1] https://www.nelnet.com/welcome (last accessed September 7, 2022)
[2] https://www.nelnet.com/identity-theft (last accessed September 7, 2022)
[3] https://www.nelnet.com/privacy-and-security (last accessed September 7, 2022)



Our Security Procedures

We are committed to providing you a useful and enjoyable online experience. We implement reasonable and appropriate physical, procedural, and electronic safeguards to protect your information.

To access information and send email via the website, you will need a browser that supports the use of Secure Sockets Layer. This encryption technology helps ensure the authenticity of your online sessions and secures data transmitted over the public Internet.

Nelnet takes careful steps to safeguard customer information. We restrict access to your personal and account information to employees who need to know the information to provide services to you, and we regularly train our employees on privacy, information security, and their obligation to protect your information. We maintain reasonable and appropriate physical, electronic, and procedural safeguards to guard your Nonpublic Personal Information (NPI) and Personally Identifiable Information (PII), and we regularly test those safeguards to maintain the appropriate levels of protection.

You can help safeguard your NPI and PII by taking a few simple precautions. Protect your account numbers, passwords, and customer access numbers. Never disclose confidential information to unknown callers. You should always use a secure browser and current virus detection software, and never open email from unknown sources.

22. Despite recognizing its duty to do so, on information and belief, Nelnet has not implemented reasonable cybersecurity safeguards or policies to protect borrower PII or trained its IT or data security consumers to prevent, detect, and stop breaches of Nelnet systems. As a result, Nelnet leaves vulnerabilities in its systems for cybercriminals to exploit and gain access to borrowers' PII.

Nelnet Fails to Safeguard Borrowers' PII

23. Plaintiff and the proposed Class are current and former borrowers whose PII was given to Nelnet in the context of student loan servicing.

24. Nelnet obtains borrowers' PII to as a condition to performing loan servicing for their loans.

25. Nelnet collects and maintains borrower PII in its computer systems.

26. In collecting and maintaining borrower PII, Nelnet implicitly agrees it will safeguard the data using reasonable means according to its internal policies, as well as state and federal law.

27. Despite its duties to safeguard PII, beginning on or around June 1, 2022, cybercriminals bypassed Nelnet's inadequate security systems undetected and accessed confidential borrower PII.

28. On or around July 22, 2022, Nelnet finally identified unusual network activity and eventually determined that cybercriminals had accessed borrowers' PII.

29. Defendant's investigation revealed that its network had been hacked by cybercriminals and that Defendant's inadequate cyber and data security systems and measures allowed those responsible for the cyberattack to obtain files containing a treasure trove of thousands of consumers' personal, private, and sensitive information, including but not limited to names, addresses, email addresses, phone numbers and Social Security numbers.

30. Consumers place value in data privacy and security. These are important considerations when deciding where and to whom consumers will disclose PII. Plaintiff would not have provided her PII to Nelnet or its affiliates had she known that Nelnet does not take all necessary precautions to secure the personal data given to it by consumers.

31. Despite its duties and alleged commitments to safeguard PII, Nelnet does not follow industry standard practices in securing consumers' PII, as evidenced by the Data Breach and stolen consumer PII.

32. In response to the Data Breach, Nelnet contends that it "took immediate action to secure the information system, block the suspicious activity, fix the issue and launched an investigation with third-party forensic experts to determine the nature and scope of the activity." However, these actions were too little, too late to prevent the Data Breach in the first place.

33. Through its Breach Notice, Nelnet also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "remain vigilant

against incidents of identity theft and fraud over the next 24 months, by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors."

34. Nelnet has offered some complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers and birth dates.

35. Even with complimentary credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

36. Cybercriminals need not harvest a person's Social Security number in order to commit identity fraud or misuse Plaintiff's and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

37. On information and belief, Nelnet failed to adequately train its IT and data security consumers on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over consumer PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing PII. Further, the Breach Notice makes clear that Nelnet cannot, or will not, determine the full scope of the Data Breach.

Plaintiff's Experience

38. Plaintiff Miller had a student loan that was serviced by Nelnet.

39. As a condition of receiving such loan servicing from Nelnet, Plaintiff entrusted Nelnet with her PII.

40. Plaintiff provided her PII to Nelnet and trusted the company would use reasonable measures to protect it according to Nelnet's internal policies, as well as state and federal law.

41. Plaintiff has and will spend considerable time and effort monitoring her is accounts to protect herself from identity theft. Plaintiff fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

Plaintiff and the Proposed Class Face Significant Risk of Identity Theft

42. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

43. The ramifications of Nelnet's failure to keep Plaintiff and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, or other information, without permission, to commit fraud or other crimes.

44. The types of personal data compromised and potentially stolen in the Nelnet Data Breach is highly valuable to identity thieves. The consumers' stolen PII can be used to gain access to a variety of existing accounts and websites to drain assets, bank accounts or open phony credit cards.

45. As a result of Nelnet's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses,

lost time, anxiety, and emotional distress. They have suffered, or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of Nelnet and is subject to further breaches so long as Nelnet fails to undertake the appropriate measures to protect the PII in their possession.

46. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.[4]

47. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen

[4] *See* Here's How Much Your Personal Information Is Selling for on the Dark Web, Experian, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited September 7, 2022).

private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

48. It can take victims years to stop identity or PII theft, giving criminals time to sell that information for cash.

49. One such example of criminals using PII for profit is the development of "Fullz" packages.

50. Cybercriminals can cross-reference multiple sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.[5]

51. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

52. Defendant disclosed the PII of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed,

[5] *Id.*

and exposed the PII of Plaintiff and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

53. Defendant's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has exposed the PII of Plaintiff and thousands of members of the proposed class to unscrupulous operators, con artists and criminals.

54. Defendant's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff's and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Nelnet Failed to Adhere to FTC Guidelines.

55. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

56. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

57. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

58. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

59. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

60. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

CLASS ACTION ALLEGATIONS

61. Plaintiff brings this action pursuant to FRCP 23(b)(2) and (b)(3) on behalf of herself and all members of the proposed national class (the "Class") tentatively defined as:

> All persons residing in the United States whose PII was compromised in the Data Breach disclosed by Nelnet in August 2022.

62. The following people are excluded from the Class: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which the Defendant or its parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

63. The Class defined above is identifiable through Defendant's business records.

64. Plaintiff reserves the right to amend the Class definition or add a Class if further information and discovery indicate that other classes should be added and if the definition of the Class should be narrowed, expanded, or otherwise modified.

65. This action satisfies the numerosity, commonality, typicality, and adequacy requirements of Fed. R. Civ. P. 23.

Numerosity

66. The exact number of Class members is unknown but is estimated to be up to thousands of consumers at this time, and individual joinder in this case is impracticable. Class Members can be easily identified through Defendant's records and objective criteria permitting self-identification in response to notice, and notice can be provided through techniques like those customarily used in other data breach, consumer breach of contract, unlawful trade practices, and class action controversies.

67. Plaintiff is a member of the Class.

Commonality

68. There are questions of law and fact common to Plaintiff and to the proposed Class, including but not limited to the following:

a. Whether Nelnet had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;

b. Whether Nelnet failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Nelnet was negligent in maintaining, protecting, and securing PII;

d. Whether Nelnet breached contract promises to safeguard Plaintiff's and the Class's PII;

e. Whether Nelnet took reasonable measures to determine the extent of the Data Breach after discovering it;

f. Whether Nelnet's Breach Notice was reasonable;

g. Whether the Data Breach caused Plaintiff and the Class injuries;

h. What the proper damages measure is; and

i. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

69. Common questions of law and fact predominate over questions affecting only individual class members, and a class action is the superior method for fair and efficient adjudication of the controversy.

70. Plaintiff's claims are typical of the claims of Class members.

Adequacy

71. Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the Class, she will fairly and adequately protect the interests of the Class, and she is represented by counsel skilled and experienced in class actions.

FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiff and the Class)

72. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

73. Plaintiff and members of the Class entrusted their PII to Defendant. Defendant owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

74. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards for data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and members of the Class's PII by disclosing and allowing access to consumer PII to unknown third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who made that happen.

75. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable time frame of any breach to the security of their PII. Defendant also owed a

duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

76. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and members of the Class's PII for purposes of loan servicing, a for-profit business. Plaintiff and members of the Class needed to provide their PII to Defendant in order to receive loan servicing from Defendant. Defendant negligently retained this information.

77. The risk that unauthorized persons would try to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would try to access Defendant's databases containing the PII—whether by ransomware or otherwise.

78. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and members of the Class and the importance of exercising reasonable care in handling it.

79. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and members of the Class which actually and proximately caused the Data Breach and Plaintiff's and members of the Class's injury.

80. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact.

81. As a direct and traceable result of Defendant's negligence or negligent supervision, Plaintiff, and members of the Class have suffered or will suffer damages, including but not limited to monetary damages, loss of privacy, lost time, loss of value of PII, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

82. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff's and members of the Class's actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CLAIM FOR RELIEF
Negligence Per Se
(On Behalf of Plaintiff and the Class)

83. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

84. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant has a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII.

85. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the members of the Class's sensitive PII. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, consumers' PII.

86. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect its consumers' PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to its consumers in the event of a breach, which ultimately came to pass.

87. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

88. Defendant had a duty to Plaintiff and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and the Class's PII.

89. Defendant breached its respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII.

90. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

91. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

92. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

93. Had Plaintiff and members of the Class known that Defendant did not adequately protect consumers' PII, Plaintiff and members of the Class would not have entrusted Defendant with their PII.

94. As a direct and proximate result of Defendant's negligence per se, Plaintiff and members of the Class have suffered harm, including loss of time and money resolving fraudulent charges loss of time and money obtaining protections against future identity theft; lost control over the value of their PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

THIRD CLAIM FOR RELIEF
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

95. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

96. Defendant and Plaintiff and members of the Class had an implied contract whereby Nelnet agreed to provide adequate data security to protect the PII of Plaintiff and the Class.

97. Through its own internal policies, Defendant agreed it would not disclose the PII it collects to unauthorized persons. Defendant also promised to safeguard consumer PII.

98. Plaintiff and the members of the Class accepted Defendant's offer by providing PII to Defendant in exchange for loan servicing.

99. Implicit in the parties' agreement was that Defendant would provide Plaintiff and members of the Class with prompt and adequate notice of all unauthorized access and/or theft of their PII.

100. Plaintiff and the members of the Class would not have entrusted their PII to Defendant in the absence of such agreement with Defendant.

101. Defendant materially breached the contracts it had entered with Plaintiff and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant also breached the implied contracts with Plaintiff and members of the Class by:

a. Failing to properly safeguard and protect Plaintiff's and members of the Class's PII;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PII that Defendant created, received, maintained, and transmitted.

102. The damages sustained by Plaintiff and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

103. Plaintiff and members of the Class have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

104. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

105. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

106. Defendant failed to advise Plaintiff and members of the Class of the Data Breach promptly and sufficiently.

107. In these and other ways, Defendant violated its duty of good faith and fair dealing.

108. Plaintiff and members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches of it through violations of the covenant of good faith and fair dealing.

109. Plaintiff, on behalf of himself and the Class, seeks compensatory damages for breach of implied contract, which includes the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

FOURTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of the Plaintiff and the Class)

110. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

111. This claim is plead in the alternative to the breach of implied contractual duty claim.

112. Plaintiff and members of the Class conferred a benefit upon Defendant in the form of paying for loan servicing through fees their lender imposed. Defendant also benefited from the receipt of Plaintiff's and members of the Class's PII, as this was used to facilitate loan servicing.

113. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and members of the Class.

114. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the proposed Class's payments and their PII because Defendant failed to adequately protect their PII. Plaintiff and the proposed Class would not have provided their PII or used Defendant for loan servicing, had they known Defendant would not adequately protect their PII.

115. Defendant should be compelled to disgorge into a common fund to benefit Plaintiff and members of the Class all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged here.

FIFTH CLAIM FOR RELIEF
Invasion of Privacy
(On Behalf of the Plaintiff and the Class)

116. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

117. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

118. Defendant owed a duty to its consumers, including Plaintiff and the Class, to keep this information confidential.

119. The unauthorized acquisition (*i.e.*, theft) by a third party of Plaintiff's and Class Members' PII is highly offensive to a reasonable person.

120. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant as part of loan servicing, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

121. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

122. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

123. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

124. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

125. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

126. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII are still maintained by Defendant with their inadequate cybersecurity system and policies.

127. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiff and the Class.

128. In addition to injunctive relief, Plaintiff, on behalf of himself and the other members of the Class, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Nelnet from further deceptive and unfair practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Class damages that include compensatory, exemplary, punitive damages, and statutory damages, including pre- and post-judgment interest, in an amount to be proven at trial;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

I. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

Dated: September 8, 2022

Respectfully submitted,

/s/ *Gary M. Klinger*

Gary M. Klinger
David K. Lietz*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
Fax: (865) 522-0049
gklinger@milberg.com
dlietz@milberg.com

Samuel J. Strauss
sam@turkestrauss.com
Raina C. Borrelli
raina@turkestrauss.com
Alex Phillips
alexp@turkestrauss.com

TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
Telephone (608) 237-1775
Facsimile: (608) 509-4423

Attorneys for Plaintiff and the Proposed Class